Project 2: Shift Register Sequences in Rust

Group 06: Fredrick Nilsson

December 1, 2023

Contents

Home Exercise 1

..

1. $p(x) = x^4 + x^2 + 1$ over $\mathbb{F}_2$

Since $x^4 + x^2 + 1 = (x^2 + x + 1)^2$ it is not irreducible, and therefore not primitive.

2. $p(x) = x^3 + x + 1$ over $\mathbb{F}_3$

Since $x^3 + x + 1 = x^3 + 3x^2 + 4x + 4 = (x + 2)(x^2 + x + 2)$, it clearly has factors and is therefore not irreducible. Since it is not irreducible, it is not primitive.

3. $p(x) = x^2 + \alpha^5 x + 1$ over $\mathbb{F}_{2^4}$, where $\alpha^4 + \alpha + 1 = 0$

If there is an i such that $p(a^i) = 0$, then $p(x)$ has a root, and is therefore not primitive nor irreducible.
If $i = 6$, then $p(\alpha^6) = \alpha^{12} + \alpha^{11} + 1 = (\alpha^3 + \alpha^2 + \alpha + 1) + (\alpha^3 + \alpha^2 + \alpha) + 1 = 2\alpha^3 + 2\alpha^2 + 2\alpha + 2 = 0$ As shown, $p(x)$ is reducible and therefore not primitive.

Lab Exercise 1

1. $p(x) = x^{23} + x^5 + 1$ over $\mathbb{F}_2$

> Primitive($x^{23} + x^5 + 1$) **mod** 2
> True

Therefore $p(x)$ is primitive, and therefore irreducible.

2. $p(x) = x^{23} + x^6 + 1$ over $\mathbb{F}_2$

> Primitive($x^{23} + x^6 + 1$) **mod** 2
> False
> Irreduc($x^{23} + x^6 + 1$) **mod** 2
> False

Therefore $p(x)$ is neither a primitive nor irreducible.

3. $p(x) = x^{18} + x^3 + 1$ over $\mathbb{F}_2$

> Primitive($x^{18} + x^3 + 1$) **mod** 2
> False
> Irreduc($x^{18} + x^3 + 1$) **mod** 2
> True

Therefore $p(x)$ is not a primitive, but it is irreducible.

4. $p(x) = x^8 + x^6 + 1$ over $\mathbb{F}_7$

> Primitive($x^8 + x^6 + 1$) **mod** 7
> False
> Irreduc($x^8 + x^6 + 1$) **mod** 7
> False

Therefore $p(x)$ is neither a primitive nor irreducible.

5. $p(x) = x^6 + \alpha^5 x + 1$ over $\mathbb{F}_{2^4}$

> G4 := GF(2, 4, $\alpha^4 + \alpha + 1$)
> G4 := $\mathbb{F}_{16}$
> x := α
> a := G4:-ConvertIn($x^6 + \alpha^5 * x + 1$)
> a := $1 \mod 2$
> x := α^2
> a := G4:-ConvertIn($x^6 + \alpha^5 * x + 1$)
> a := $\alpha^2 + 1 \mod 2$
> x := α^3

...

> x := α^{14}
> a := G4:-ConvertIn($x^6 + \alpha^5 * x + 1$)
> a := $\alpha^3 \mod 2$
> G4:-isPrimitiveElement(a)
> false

Since the function wasn't evaluated to 0 for any of the α^i, $p(x)$ is irreducible. But is not primitive.

Home Exercise 2

$|\mathbb{F}_{2^4}| = 16 \implies \alpha^{15} \equiv 1$, therefore the possible orders for a polynomial consisting of one α are all possible factors of 15, that is 1, 3, 5 and 15.

1. α

$ord(\alpha) = n \implies \alpha^n \equiv \alpha^{15} \implies n = 15.$ The order of α is 15.

2. α^2

$ord(\alpha) = n \implies \alpha^{2n} \equiv \alpha^{15} \implies n = 15.$ The order of α is 15.

3. α^3

$ord(\alpha) = n \implies \alpha^{3n} \equiv \alpha^{15} \implies n = 5.$ The order of α is 5.

4. α^5

$ord(\alpha) = n \implies \alpha^{5n} \equiv \alpha^{15} \implies n = 3.$ The order of α is 3.

Lab Exercise 2

```
> G18 := GF(2, 18, α^18 + α^3 + 1)
> G18 := 𝔽_{2^18}
```

1. α

```
> a := G18:-ConvertIn(α);
> ...
> G18:-order(a)
> 189
```

2. α^2

```
> a := G18:-ConvertIn(α^2);
> ...
```

```
> G18:-order(a)
> 189
```

3. α^3

```
> a := G18:-ConvertIn(α^3);
> ...
> G18:-order(a)
> 63
```

4. $\alpha + \alpha^3$

```
> a := G18:-ConvertIn(α+α^3);
> ...
> G18:-order(a)
> 262143
```

Home Exercise 3

1. $p(x) = x^4 + x^2 + 1$ over $\mathbb{F}_2$

Since $x^4 + x^2 + 1 = (x^2 + x + 1)^2$ we can describe $C(D) = C_1(D)^n$, where $C(D) = (1 + D + D^2)^2$ and $C_1(D) = 1 + D + D^2$ with $n = 2$. Therefore we can calculate $L_1 = \deg C_1(D) = 2$, with the period $T_1 = 3$ of C_1. We can then calculate $T_2 = p^m T_1 = 2^1 2 = 4$, with $m = 1$ since $2^0 < 2 \leq 2^1$. We can then plug these numbers into the formula $1(1) \oplus \frac{q^{L_1}-1}{T_1}(T_1) \oplus \frac{q^{L_1}(q^{L_1}-1)}{T_2}(T_2)$. Which results in the cycle set $1(1) \oplus 1(3) \oplus 2(6)$.

2. $p(x) = x^3 + x + 1$ over $\mathbb{F}_3$

Since $x^3+x+1 = (x+2)(x^2+x+2)$ we can describe $C(D) = C_1(D) * C_2(D)$, where $C(D) = D^3 + D + 1$, $C_1(D) = D + 2$ and $D^2 + D + 2$. We can see that the order of C_1, $T_{1_1} = 1$ since

$$1 = 2(D + 2) + (-2D)$$

We can also see that the order of C_2, $T_{2_1} = 8$ since

$$
\begin{aligned}
1 &= 2(D^2 + D + 2) + (-2D^2 - 2D) \\
1 &= (2 + 2D)(D^2 + D + 2) + (-2D^3 - D^2) \\
1 &= (2 + 2D + D^2)(D^2 + D + 2) + (-D^4) \\
1 &= (2 + 2D + D^2 + D^4)(D^2 + D + 2) + (-D^6 - D^5) \\
1 &= (2 + 2D + D^2 + D^4)(D^2 + D + 2) + (-D^6 - D^5) \\
1 &= (2 + 2D + D^2 + D^4 + D^5)(D^2 + D + 2) + (-D^7 - 2D^6) \\
1 &= (2 + 2D + D^2 + D^4 + D^5 + 2D^6)(D^2 + D + 2) + (-2D^8)
\end{aligned}
$$

We can then plug these numbers into the formula $1(1) \oplus \frac{q^{L_1} - 1}{T_1}(T_1) \oplus \frac{q^{L_1}(q^{L_1} - 1)}{T_2}(T_2)$. Which results in the cycle set $1(1) \oplus 2(1)$ for C_1, and the cycle set $1(1) \oplus 1(8)$ for C_2. Resulting in the cycle set $(1(1) \oplus 2(1)) \times (1(1) \oplus 1(8)) = 1(1) \oplus 1(8) \oplus 2(1) \oplus 2(8) = 3(1) \oplus 3(8)$ for $C(D)$.

Lab Exercise 3

1. $p(x) = x^{23} + x^5 + 1$ over $\mathbb{F}_2$

Calculate the order through: `> G23 := GF(2, 23,` $\alpha^{23} + \alpha^5 + 1$`)`

`> G23 :=` $\mathbb{F}_{2^{23}}$

`> a := G23:-ConvertIn(`α`)`

`> a :=` $\alpha \mod 2$

`> G23:-order(a)`

`> 8388607`

With the order $T_1 = 8388607$, we can calculate the cycle set through the formula $1(1) \oplus \frac{q^{L_1} - 1}{T_1}(T_1) \oplus \frac{q^{L_1}(q^{L_1} - 1)}{T_2}(T_2)$. Resulting in a cycle set of $1(1) \oplus 1(8388607)$.

2. $p(x) = x^{23} + x^6 + 1$ over $\mathbb{F}_2$

`> Factor(`$x^{23} + x^6 + 1$`) mod 2;`

`>` $(x^4 + x^3 + 1) \times (x^{16} + x^{15} + x^{13} + x^{12} + x^8 + x^6 + x^4 + x^3 + x^2 + x + 1) \times (x^3 + x + 1)$

Which gives us the three polynomials $C_1(D) = D^4 + D^3 + 1$, $C_2(D) = D^{16} + D^{15} + D^{13} + D^{12} + D^8 + D^6 + D^4 + D^3 + D^2 + D + 1$ and $C_3(D) = D^3 + D + 1$.

We can then calculate the order of C_1, $T_1 = 15$ through:

> G4 := GF(2, 4, $\alpha^4 + \alpha^3 + 1$)
> G4 := $\mathbb{F}_{16}$
> a := G4:-ConvertIn(α)
> a := $\alpha \mod 2$
> G4:-order(a)
> 15

We can then calculate the order of C_2, $T_2 = 21845$ through:

> G16 := GF(2, 16, $\alpha^{16} + \alpha^{15} + \alpha^{13} + \alpha^{12} + \alpha^8 + \alpha^6 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$)
> G16 := $\mathbb{F}_{2^{16}}$
> a := G16:-ConvertIn(α)
> a := $\alpha \mod 2$
> G16:-order(a)
> 21845

And lastly we can calculate the order of C_3, $T_3 = 7$ through:

> G3 := GF(2, 3, $\alpha^3 + \alpha + 1$)
> G3 := $\mathbb{F}_8$
> a := G3:-ConvertIn(α)
> a := $\alpha \mod 2$
> G3:-order(a)
> 7

With these number we can calculate the cycle sets through the formula $1(1) \oplus \frac{q^{L_1}-1}{T_1}(T_1) \oplus \frac{q^{L_1}(q^{L_1}-1)}{T_2}(T_2)$. Resulting in the cycle set $1(1) \oplus 1(15)$ for C_1, $1(1) \oplus 3(21845)$ for C_2 and $1(1) \oplus 1(7)$ for C_3. Meaning we can calculate the cycle set of $C(D)$ through $(1(1) \oplus 1(15)) \times (1(1) \oplus 3(21845)) \times (1(1) \oplus 1(7)) = 1(1) \oplus 1(7) \oplus 3(21845) \oplus 3(152915) \oplus 1(15) \oplus 1(105) \oplus 3(327675) \oplus 3(2293725)$

Home Exercise 4

One primitive of degree 4 over $\mathbb{F}_2$ is $x^4 + x^3 + 1$. As it satisfies $P(0) = P(1) = 1$ and it doesn't have any factors.

Lab Exercise 4

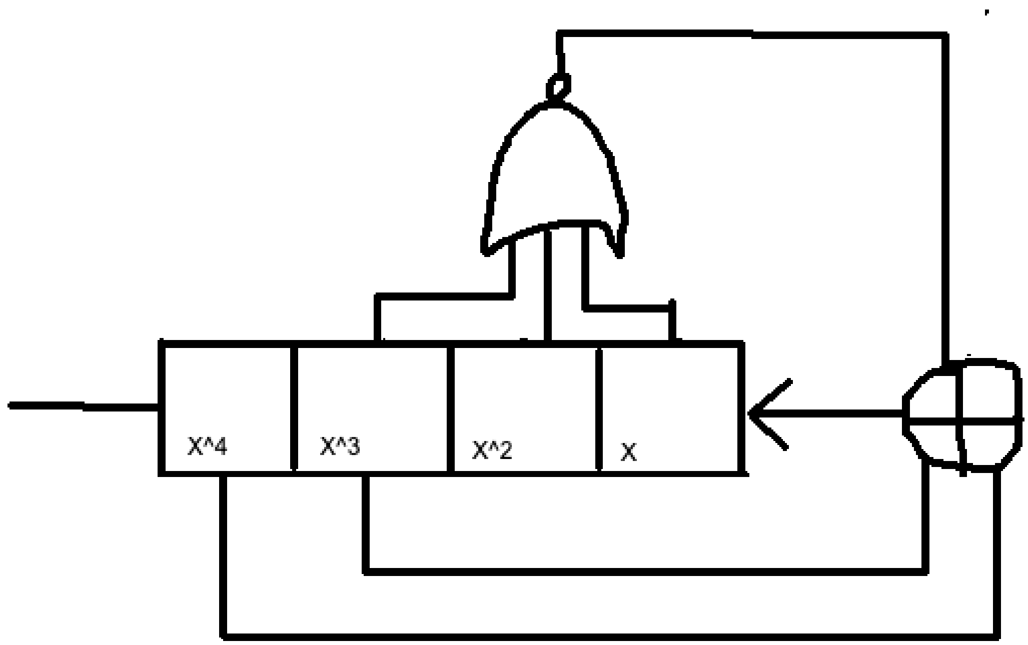
One way to find primtive polynomials is to simply iterate through all possible polynomials and filter them based on if they are primitive. This can be achieved through the following code:

```
> for i from 0 to 4 do
    for j from 0 to 4 do
      for k from 0 to 4 do
        for l from 0 to 4 do
          if (Primitive(l*x^4+k*x^3+j*x^2+i*x+1) mod 2)
            then print(l, k, j, i, 1) break
          end if
        end do
      end do
    end do
  end do
> 2, 2, 1, 0, 1
```

So one example of a primitive polynomial of degree 4 over $\mathbb{F}_5$ is $2x^4 + 2x^3 + x^2 + 1$.

Home Exercise 5

In order to generate a basic de Bruijne sequence of the format $...s \to s'...$ we can use just a simple XOR operation between over the x^4 and x^3 slots, resulting in the 16-length de Bruijn 1100010011010111. But it doesn't include the 0 state, so in order to insert it we add a simple NOR check between the x^3, x^2 and x slots, changing the sequence of states from $... \to 1000 \to 0001 \to ...$ to $... \to 1000 \to 0000 \to 0001 \to ...$, making the sequence into a $...s \to 0 \to s'...$ sequence. The resulting de Bruijn sequence of length 16 starting from $x^4 + x^3 + 1$ is 1100001001101011.



Lab Exercise 5

The program is a fairly simple implementation in rust, where it simply generates two different sequences, one for $\mathbb{Z}_2$ based on the the home assignment, and one for $\mathbb{Z}_5$. It then combines them into a single sequence, creating a de Bruijn sequence of $\mathbb{Z}_{10}$ and prints it out.

So it simply generetes two start vectors, both with the values [0,0,0,1] at line 8 and 9. These are then iterated through a loop 10003 times in order to generate their sequences. For the $\mathbb{Z}_2$ sequence, it simply adds the slots together based on the primitive $x^4 + x^3 + 1$ and reduces them to modulo 2, and then appends the result to the sequence, except in the special cases of [1,0,0,0] and [0,0,0,0], where we have special conditions for in order to add the 0 element, that is $...s \to 0 \to s'....$ The code for this can be seen on line 13-21.
For the $\mathbb{Z}_5$ sequence, it simply adds the slots together based on the primitive $2x^4 + 2x^3 + x^2 + 1$ and reduces them to modulo 5, and then appends the result to the sequence, except in the special case of [2,0,0,0] and [0,0,0,0], the reasoning for choicing these specific numbers is as the linear implemen-

tation would go through $[2,0,0,0] \rightarrow [0,0,0,1]$, resetting the cycle, therefore we add the 0 element, [0,0,0,0], inbetween these, creating the cycle ... $\rightarrow$ 2000 $\rightarrow$ 0000 $\rightarrow$ 0001 $\rightarrow$ .... The code for this can be seen on line 23-30.

The $\mathbb{Z}_{10}$ sequence is then created by adding these two sequences together and then printing them out. The code for this can be seen on line 35-44.

Source code

```
1  use std::io::*;
2
3  fn main() {
4      exercise5();
5  }
6
7  fn exercise5() {
8      let mut z2 = vec![0, 0, 0, 1];
9      let mut z5 = vec![0, 0, 0, 1];
10     // create file sequence.txt
11     for i in 0..10003 {
12         z2.push(
13             match z2.clone()[i..] {
14                 // Special case of 1000->0000->0001
15                 [0, 0, 0, 0] => 1,
16                 [1, 0, 0, 0] => 0,
17                 // General case x^4 + x^3 + 1
18                 [a,b,_,_] => (-(a+b) as i32).rem_euclid(2),
19                 _ => unreachable!()
20             }
21         );
22         z5.push(
23             match z5.clone()[i..] {
24                 // Special case of 2000->0000->0001
25                 [0, 0, 0, 0] => 1,
26                 [2, 0, 0, 0] => 0,
27                 // General case 2x^4 + 2x^3 + x^2 + 1
```

```
                [a,b,c, _] => (-(2*a+2*b+c) as i32).rem_euclid(5),
                _ => unreachable!()
            }
        );
    }
    // print to file
    let mut file = std::fs::File::create("output.txt").unwrap();
    file.write_all(
        z2.iter().zip(z5.iter()).skip(4)
        .map(|(a,b)| {
            return (5*a + b).to_string();
        })
        .reduce(|a,b|
            a + "\n" + &b
        ).unwrap().as_bytes()
    ).unwrap();
}
```

de Bruijn sequence $\mathbb{Z}_{10}$

048947276564243902650936958044084457452858514347246827087872334744
990547657412282486052888701008326648279880331621980717579424291476
371599930118235707195552031834992528986304250367351588513309309606
078684432644564649668433380089254879914317009616457551142731993615
667242360479093898932347147538365771410904780509567113384096362658
900129107516076653103702591718869233073288271866610018408648378674
003722854507789412381275274989620348036636369684234511670947875303
460058074776613037129706355793204522592706756404082476173966541416
447627275571301731691748556444153059463879612445448818295681012712
673718968022290389190656820005109849277651424840760548695304453495
290785801439229637258782233924994509765241273298150788820105337619
377983033612693526757442474197182659943016328525269550203633994707
898130470086280658801335435915157863443714951919966343383058470987
941436205916195750114723694816566224281097454889843239219708386572
141540973505956211383459181765840017415706157660310820754626886423
352378372686611006345819387862400822780905778441283177072998912039

3086181869634239016625497870303910553529776113082179251855743209027547256751404532971628966041461497172775521306236646298551444603554918879112490498363795631017217628268963022740884645656320050159394777601429345715098690304903990745785301484279182758732238429949059760241723793605788320150387164877933038117648076752442924692637659443061378070769500208138949257893130920581735658301380485460657813448219906469961343833553925987441481255461695700119228649366561224731592909889343284269253886522146045928055951211833954636765340062465251657610315325709176881423802873827686111051395364887812405327735455773441733672527998412084358163686913428406617099782030841550807977111353267470685524325407709275670140903792617896104191199262777502135128619179850144910850946887411294099381879513106226717376891302724583919565132050065484977710147439526059864030940894529578030193477463775823228347949455971024622874815578332060088261987743308316719357670244742964718765444351187352576900025318849475784313542553628565330183098091565731349326945196991134833850847598244193175091669520016427819486651122923654745988434373476470888602219109547355590121633890918676034051296070665711036037525467683142830782837768111150189081988731245037728095572344623862707799341253485361868641347345616259973203534650535797211180376292568502437045725477562014540874716789110464169471777700218017816467980014941580549688241174459483687901315127626287684130722953846956013250056093997721019248907155981403544584907957303064397291877532327339749495592102912782936557333251058371698724335336626485762024924791926876044480168280757640007036839497573431804750817856033063359354656523139437649069694113933880539759324464367054666902006147736498660112742860929598343482397192588810226415909285554012613884546867103450179152566521108108707096763314733573738776311160068453698823129008727359552234912881725779434170398081686814139239516175992320803960508579221163087174756800248209527097751201904582926678411091466492677720026306736196793001944653509968324162495493868740136017717178763413522790839695101370055154899722106429845265593140804953945795230351489274687703237238929499554210741773748655233370155382669822438038617198571202942974647687104493066373575714005208638499752343630970536785103351385480965602318448719456964411843883508975432491486250966640205119728199861011724781547959334393289264758831027146545478550401711883909686210390067460756602115315825259671331923852828877131161056390869832317405827285950223941783627577443462089353668631

141842890616759423253089150585742216135826297563002932590725977012
0640953747667341154196194767772200713562816967430064496080599633246
129909488682401810672626787134180277453896901018205506098992221514
793907655431453099084957902308019847296872032822884749995042152467
282986502338206508376693224830881626985212074479291976821049435618
285752140502581839997023481359250867801038018809359651023634982649
569144163488380589704329419817059661402501692736998110162297360979
543348437847197583310721960909785004062168384596812108405629157561
021603653707596213364288073788721316115518458693323624553727859002
284467381775724439125848086681314634784516675442370358460558524226
118537179751300743754527597201251459082976623416046916497672220521
851736696243051499153559913329117945498863240631562717678213463077
290889640106325505159894222601974845765043190359453995740235306939
279682203732783929999004260296273798600238325605387664322933583617
698021252497474697632109448516378570214500753638999202393185470586
730108306835485960102813993719956414461398383558920437446936255961
140700664728699311061279281597904339348739269753331522691545978000
451266383959631215345517465751102610860825759121381478352878822136
116506395864332812950827785400273496283677522448417539358663131913
973906667044282085391555802427116808267970130524870907759220170195
453797612346109646199762222502680628669124350199460855941337416749
099881324513651726767321391357274588914015137505065984422710692939
576004364085490899524028035648477963220823773847999400471079172879
810028337515088761432743853816769302170299292969713215449806187852
021900570818899420284368092558623015335638098591010731894826995141
491189383855842048249648175591114520561927869431151177473659740438
439828476970333602764609597300090176183895913126039506296570110711
581537575412183197380787832218116605189581433731790537778040072399
173867702249346708485861313641892845666204473258084655530247216635
376792013502982545775422062069090879711239115919169971222700763517
866412480069491585544138246629459983132901860627676232184185272958
841406018705056593442721564748957100481458094589902407308519397791
322532872839799440092157462787931007338706058871143724880836676430
262079474796921326049935168780202640552536889442073486354755812306
038518359854101523684937699014194168483885534209329919367554111902
551647786443160167292865924048348937397692033810771915959230054067
163889541317108905179652011521653608757041263369283578733226316615
068953143823674508777304052289462886720229439625398581131814684739

5661204923753539655030292266180876742018007937095770422512564545587
9211284165464669921227205718067861412930564946585044183296174959993
3137406815177671232634680727958341451068250556543447226519298952210
0931953549589402452358064897741327037827389794440542652917787431005
2388251558821148229835386671430712574929796421371099480668730207714
5507086884442523981809755312351088063859804106028639487694014644466
3938885034254379464867504116407506197781443610662747865424093398448
2897642038315726465954230504562618889041362158450679602016026608815
8752041713864738578233271366160568903148328629058772304502784917788
6220274489170898531136319639289561120942870808965003074276163587762
4206305748259572042701751909587421173466091966942127225526356781114
1743551949658004463379162995943318245636067762123713963527795334419
0156370555604349227606479890210543690809958440290285351989724137720
8737288974444504760746778243150288370655832119327938088662143521775
2947979142182159493566823025219505258683444702893635975031280158835
1885930415107818498764401914961848888003470487491986700416145705516
9773144811561729786042454389393789714208336527196590423500951716888
8404181265390567910206107615365870204621881928857323372186161556884
0319337817455872230900773946788122072498462589803118136918478951111
2544782535896000352477161858712425135529375952204720670645958242216
2396154696644217227507185673114624850649965300491387461799544336632
9518156771212821891807779033464065182555510439427715197984021504886
4535995344074078080698922418225828278892444900971529677324360078838
2565533216437748358861214802670749797414263265494856632307026905007
5863344920784818597003173065380688543046015736399871440641991639888
8300392098294698620046119525066972314931651627978104290488484878992
1425338607269654042800590626688340463176084556741025115716086582202
0912683647885232382268161655634036438736295582223540572849678312225
2299391758930316318646397890111704973708589100080297261685821247701
8507487590220922562519595324261289160969614426227705268562311912988
0519996030094188291679904438137906365672121732684635777403391456006
3755501048447726069793402600981908599034452457353569842246327537737
7884244940592607967232481057383756503326148729385881121930762529997
9241471376094985613235207645057581334942573936859200362356083568880
4309106528189982144514694618988330084259374969812009116907056692223
1943660617797310474098393987842147038815276960404730554517668334009
1367153955624107016526158653202541763819788023283276361665513408814
8828179553222804552739967331270279484675843036136819189784011620999

2825858410053079271668532129206805298754022542751706959032471178461596911447127725076851231641793506999103054468374667940448318745186562212623763918577240384195151875500109349727156974340710593645859403490295280856934229137708287783424944554715796223293155283875600337119827488583112643571707997424192187154998511328025719055753133944752848685420081285153856830435415607368993214901964916898333053475482996931205416645255664223644861516779231092459384898734219208836077691040923550906766333454186260895512415206607165860320704671836978302373377181666501345319837367950322730950728996233172077493967534308118636468973401612594737585341050357472666803217425635079870402704770625695403292167391659641149217727057680123614674805699410350496382966744049336829068651221712871846857224083469060687500015439927265692434521554819585440394079073585643427418725378773342944950926579122374365073887510038216937298853311714852625799242464268260999801137307526455570313844970739868042053178060885633048046515286894321940691946689333350397093799643125046619075561422814981606677423154295483989823426425838157764104542850545676133390468171589501246025615266581032520962638697330282387263666600139036938286790032723590527899123362257294896703435316818196892340611754928758034150085292766630326247518057982040720972517569040374266284665914119426727255763012811962935569441080099183796624409438637456860122621782639685222453396451568700006048